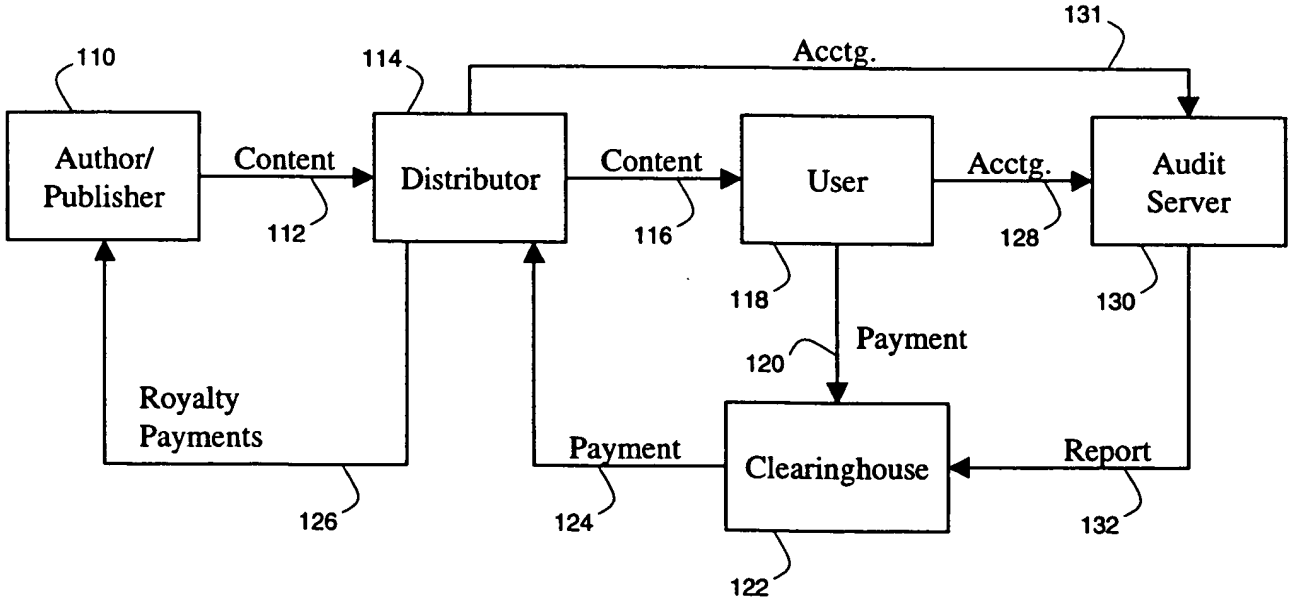
110
114
131
Acctg.
Author/
Publisher
Content
Distributor
Content
User
Acctg.
Audit
Server
112
116
128
118
130
120
Payment
Royalty
Payments
Payment
Clearinghouse
Report
126
124
132
122

Fig. 1

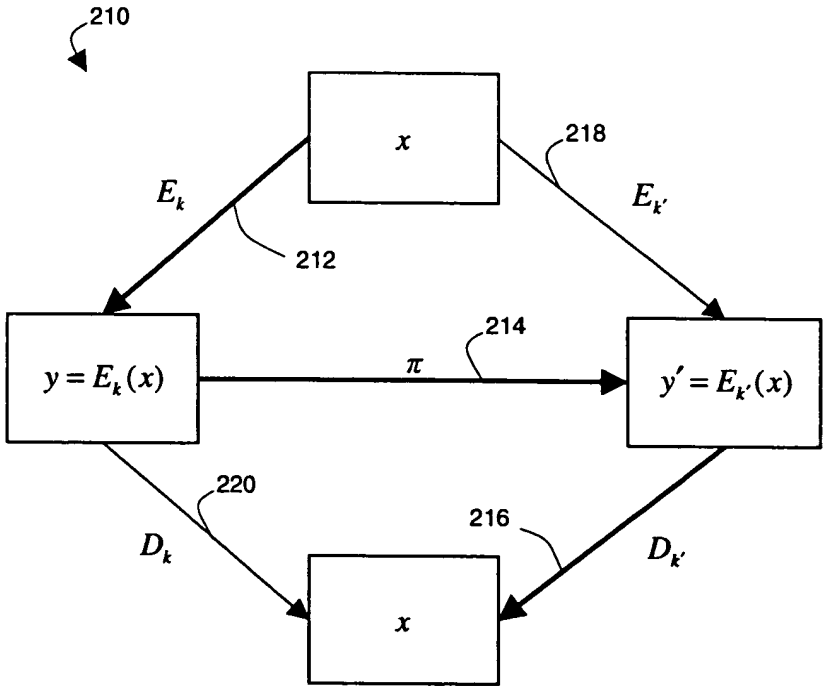

Fig. 2

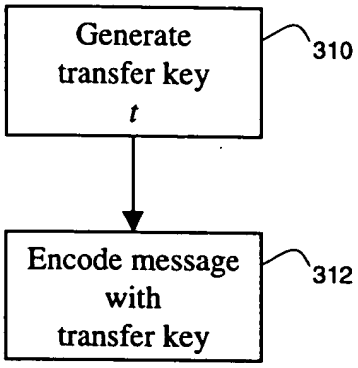
Generate transfer key t
310
Encode message with transfer key
312

Fig. 3

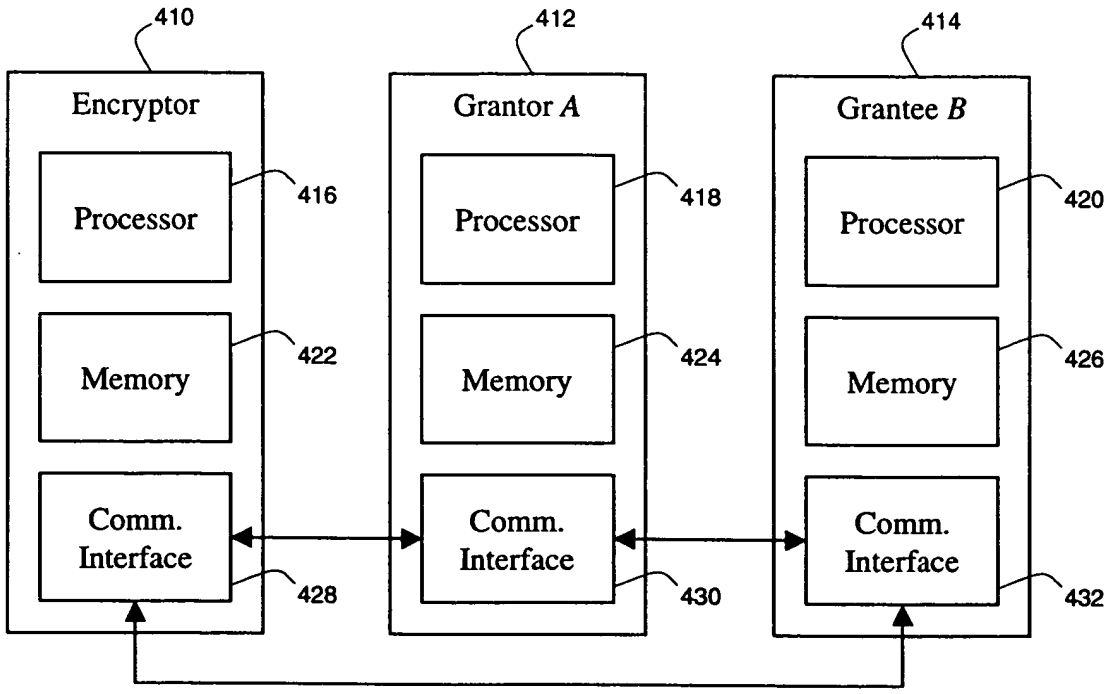
410
412
414
Encryptor
Grantor A
Grantee B
Processor
Processor
Processor
416
418
420
Memory
Memory
Memory
422
424
426
Comm. Interface
Comm. Interface
Comm. Interface
428
430
432

Fig. 4

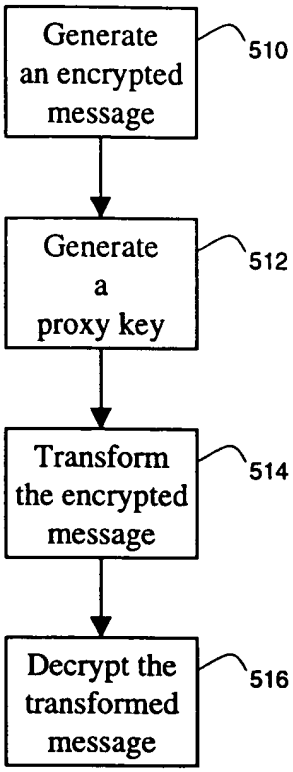
Generate an encrypted message
510
Generate a proxy key
512
Transform the encrypted message
514
Decrypt the transformed message
516

Fig. 5

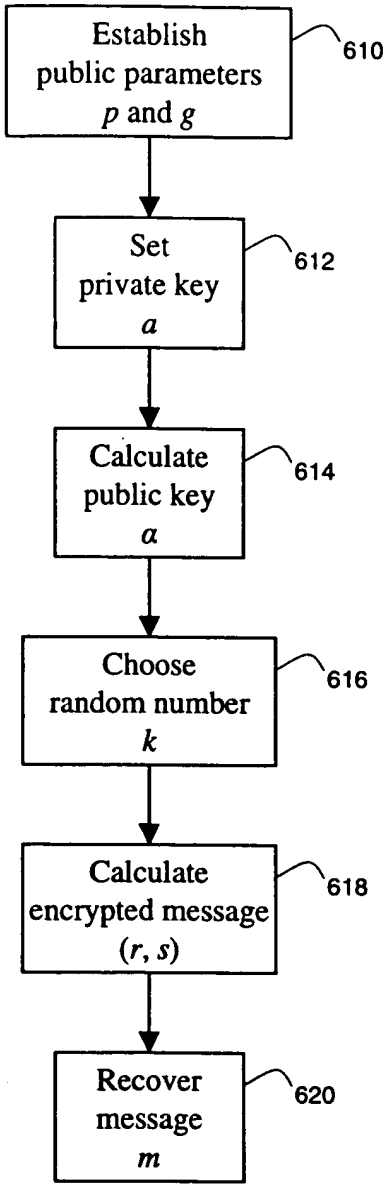
Establish public parameters p and g
610
Set private key a
612
Calculate public key a
614
Choose random number k
616
Calculate encrypted message (r, s)
618
Recover message m
620

Fig. 6

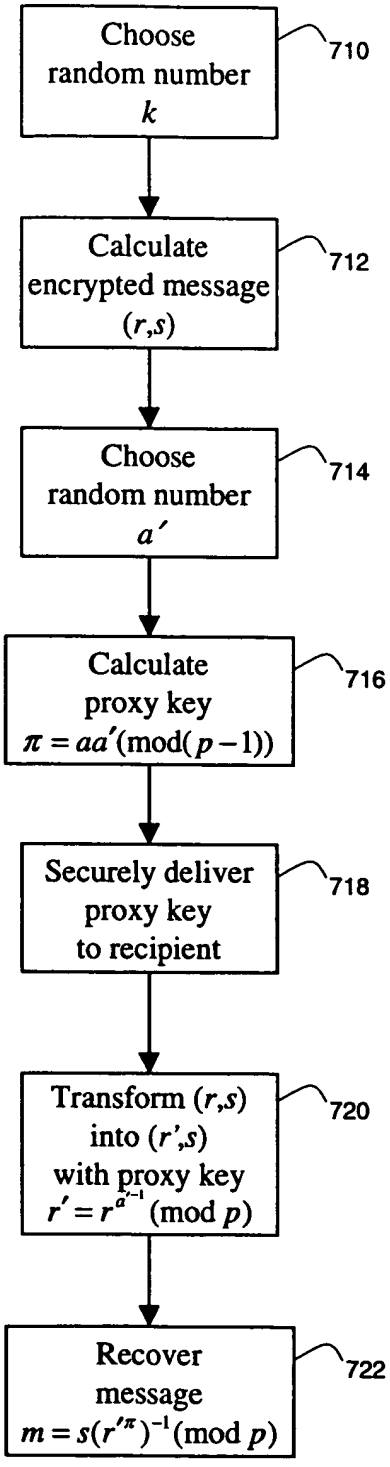
Choose random number k
710
Calculate encrypted message (r,s)
712
Choose random number a'
714
Calculate proxy key $\pi = aa'(\mathrm{mod}(p-1))$
716
Securely deliver proxy key to recipient
718
Transform (r,s) into (r',s) with proxy key $r' = r^{a'^{-1}} (\mathrm{mod}\ p)$
720
Recover message $m = s(r'^{\pi})^{-1}(\mathrm{mod}\ p)$
722

Fig. 7

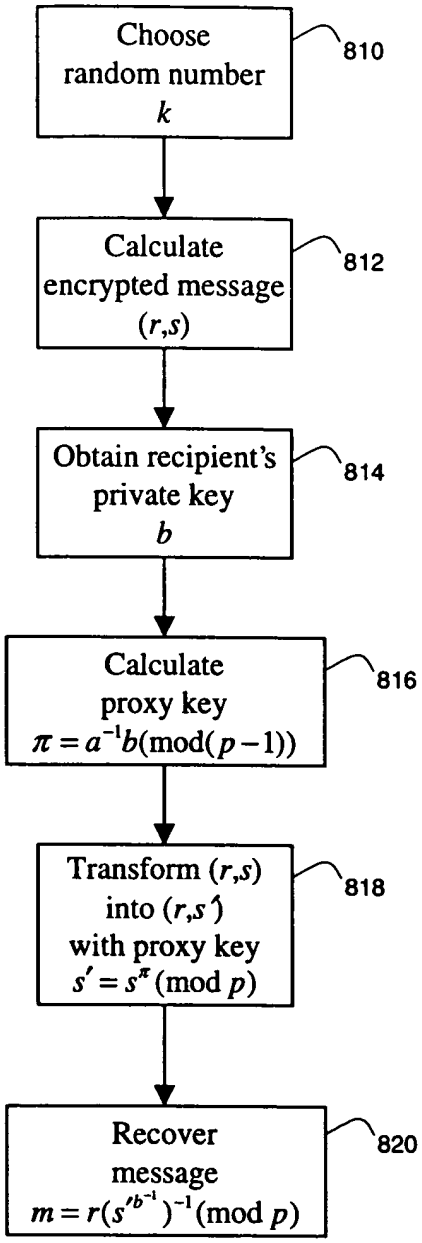
Choose random number k
810
Calculate encrypted message (r,s)
812
Obtain recipient's private key b
814
Calculate proxy key $\pi = a^{-1}b(\mathrm{mod}(p-1))$
816
Transform (r,s) into (r,s') with proxy key $s' = s^{\pi}(\mathrm{mod}\ p)$
818
Recover message $m = r(s'^{b^{-1}})^{-1}(\mathrm{mod}\ p)$
820

Fig. 8

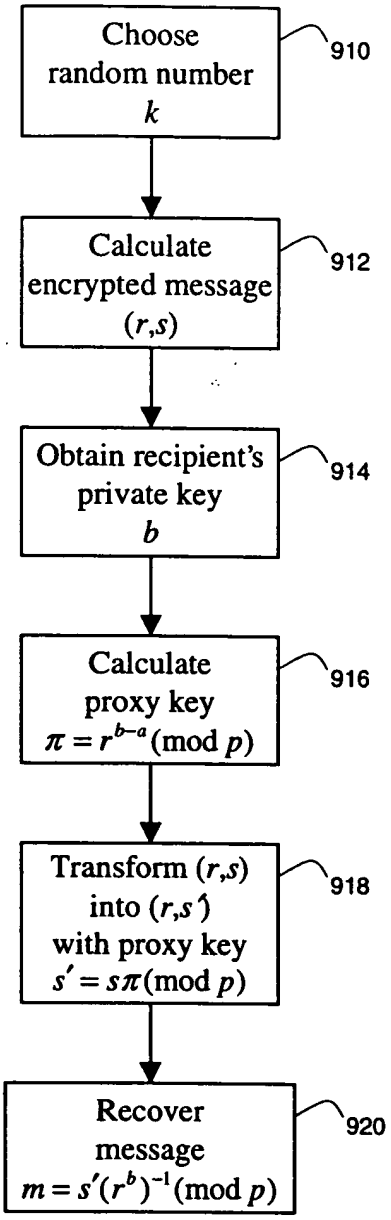
Choose random number k
910
Calculate encrypted message (r,s)
912
Obtain recipient's private key b
914
Calculate proxy key $\pi = r^{b-a} \pmod{p}$
916
Transform (r,s) into (r,s') with proxy key $s' = s\pi \pmod{p}$
918
Recover message $m = s'(r^b)^{-1} \pmod{p}$
920

Fig. 9

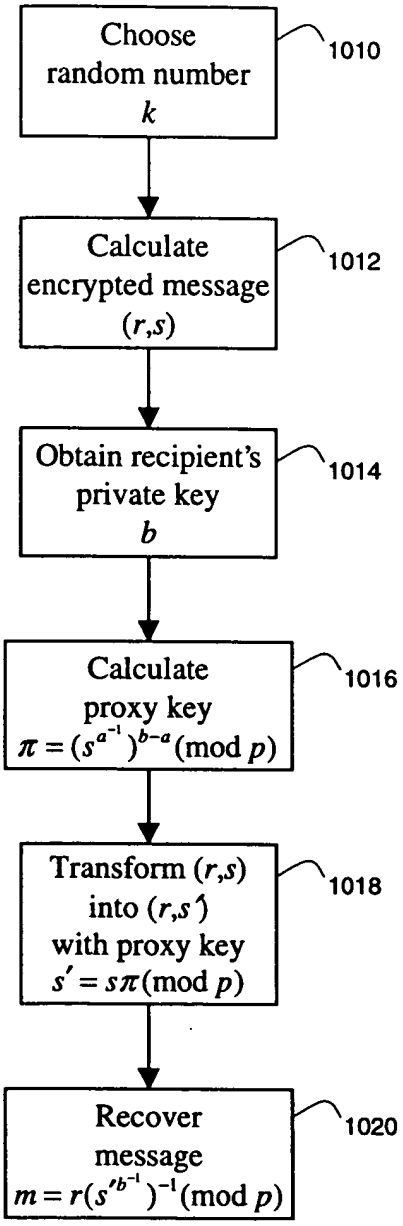
Choose random number k
1010
Calculate encrypted message (r,s)
1012
Obtain recipient's private key b
1014
Calculate proxy key $\pi = (s^{a^{-1}})^{b-a} \pmod{p}$
1016
Transform (r,s) into (r,s') with proxy key $s' = s\pi \pmod{p}$
1018
Recover message $m = r(s'^{b^{-1}})^{-1} \pmod{p}$
1020

Fig. 10

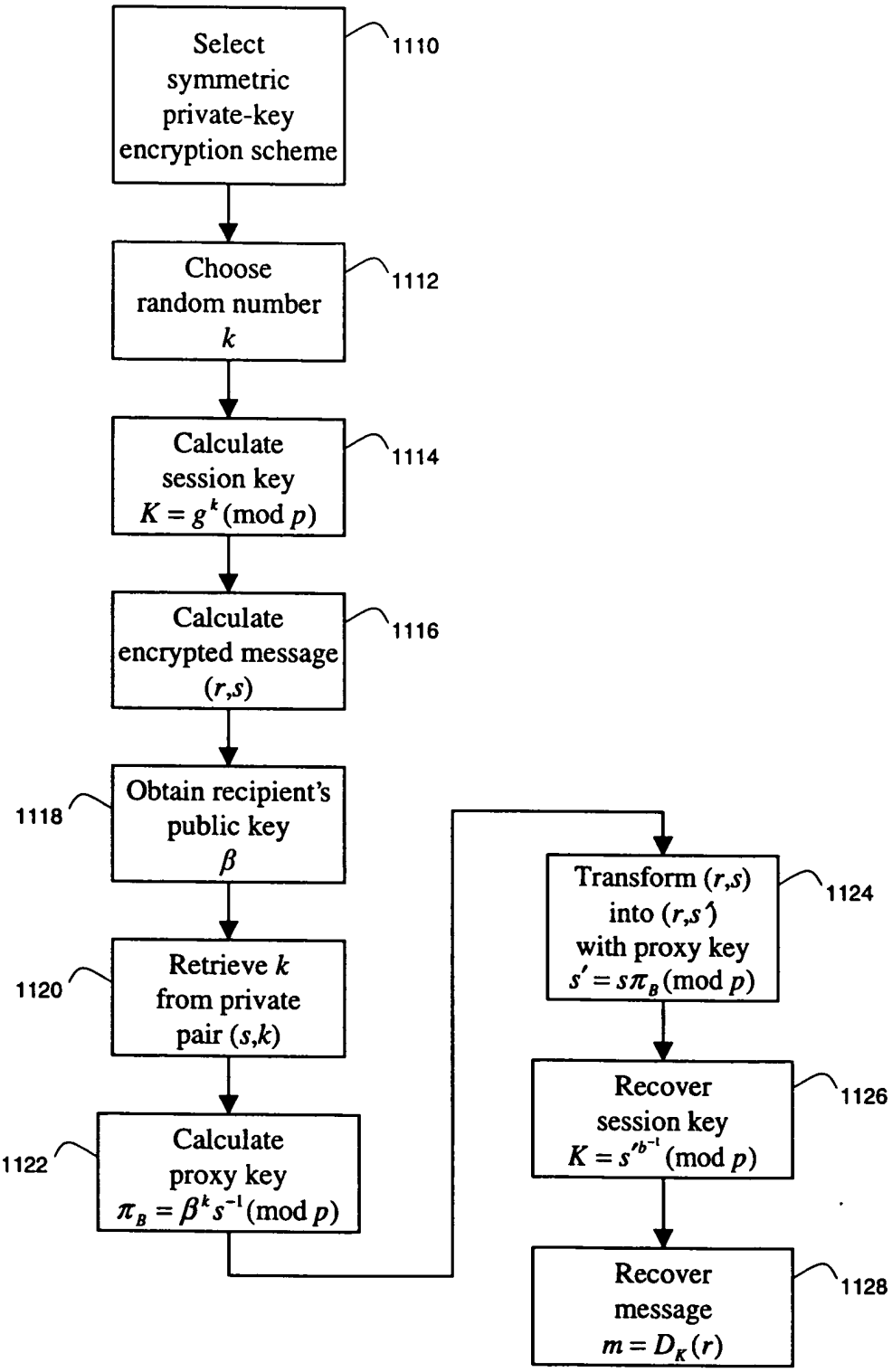
Select symmetric private-key encryption scheme
1110
Choose random number k
1112
Calculate session key $K = g^k \pmod p$
1114
Calculate encrypted message (r,s)
1116
Obtain recipient's public key β
1118
Retrieve k from private pair (s,k)
1120
Calculate proxy key $\pi_B = \beta^k s^{-1} \pmod p$
1122
Transform (r,s) into (r,s') with proxy key $s' = s\pi_B \pmod p$
1124
Recover session key $K = s'^{b^{-1}} \pmod p$
1126
Recover message $m = D_K(r)$
1128

Fig. 11

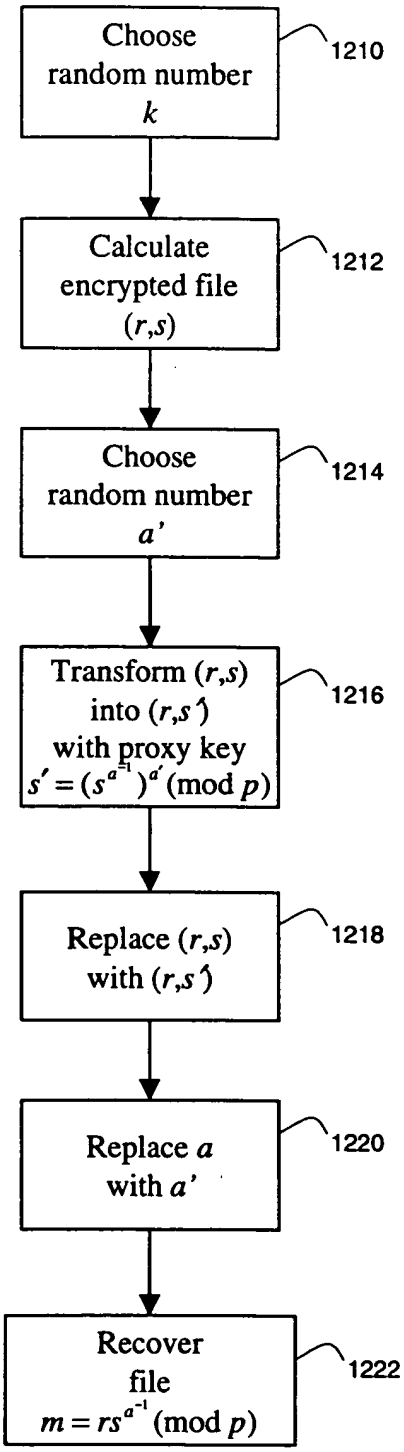
Choose random number k
1210
Calculate encrypted file (r,s)
1212
Choose random number a'
1214
Transform (r,s) into (r,s') with proxy key $s' = (s^{a^{-1}})^{a'} \pmod{p}$
1216
Replace (r,s) with (r,s')
1218
Replace a with a'
1220
Recover file $m = rs^{a^{-1}} \pmod{p}$
1222

Fig. 12

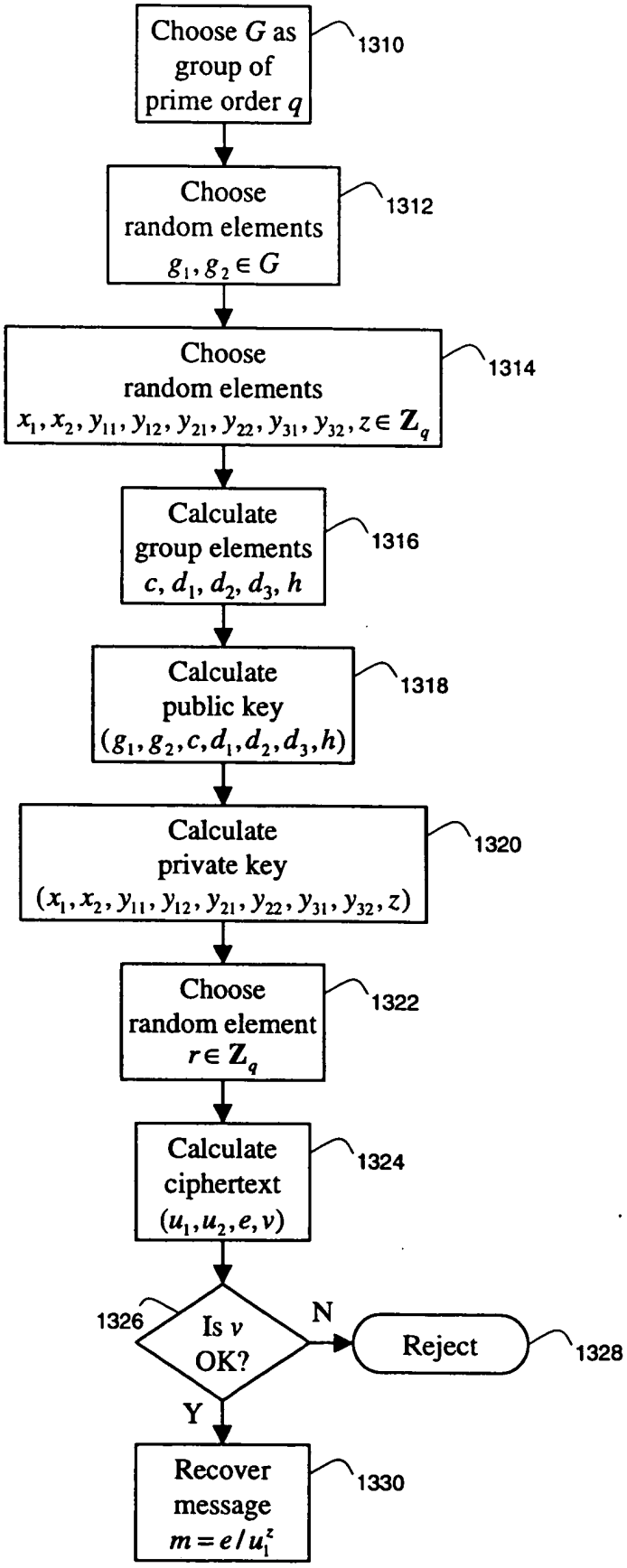
Choose G as group of prime order q
1310
Choose random elements $g_1, g_2 \in G$
1312
Choose random elements $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, y_{31}, y_{32}, z \in \mathbf{Z}_q$
1314
Calculate group elements c, d_1, d_2, d_3, h
1316
Calculate public key $(g_1, g_2, c, d_1, d_2, d_3, h)$
1318
Calculate private key $(x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, y_{31}, y_{32}, z)$
1320
Choose random element $r \in \mathbf{Z}_q$
1322
Calculate ciphertext (u_1, u_2, e, v)
1324
1326
Is v OK?
N
Reject
1328
Y
Recover message $m = e / u_1^z$
1330

Fig. 13

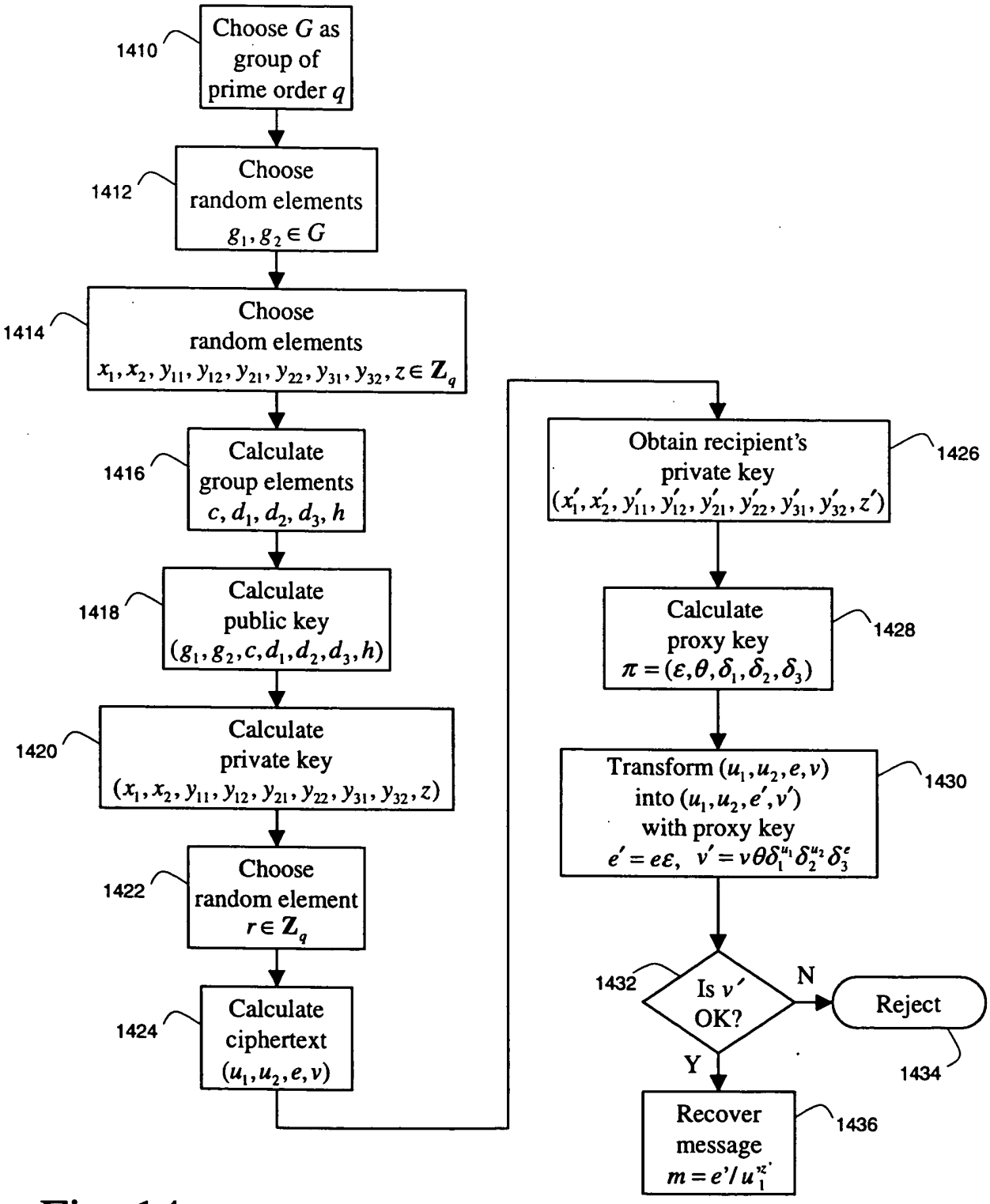
1410
Choose G as group of prime order q
1412
Choose random elements $g_1, g_2 \in G$
1414
Choose random elements $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, y_{31}, y_{32}, z \in \mathbf{Z}_q$
1416
Calculate group elements c, d_1, d_2, d_3, h
1418
Calculate public key $(g_1, g_2, c, d_1, d_2, d_3, h)$
1420
Calculate private key $(x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, y_{31}, y_{32}, z)$
1422
Choose random element $r \in \mathbf{Z}_q$
1424
Calculate ciphertext (u_1, u_2, e, v)
1426
Obtain recipient's private key $(x_1', x_2', y_{11}', y_{12}', y_{21}', y_{22}', y_{31}', y_{32}', z')$
1428
Calculate proxy key $\pi = (\varepsilon, \theta, \delta_1, \delta_2, \delta_3)$
1430
Transform (u_1, u_2, e, v) into (u_1, u_2, e', v') with proxy key $e' = e\varepsilon, \quad v' = v\theta\delta_1^{u_1}\delta_2^{u_2}\delta_3^{e}$
1432
Is v' OK?
N
Reject
1434
Y
Recover message $m = e'/u_1^{xz'}$
1436

Fig. 14